REMARKS

Initially, Applicant notes that the remarks and amendments made in this response are consistent with those presented to the Examiner by telephone.

By this paper, claims 24, 34 and 36 have been amended, and no claims have been added or canceled, such that claims 24-32, 34, and 36 remain pending, of which claims 24 and 34 are the only independent claims at issue. It will be noted that the amendments to the claims merely correct typographical errors objected to in the most recent Office Action and do not alter the claimed subject matter.

The Office Action, mailed July 1, 2008, considered and rejected claims 24-32, 34, and 36. Claims 34 and 36 were objected to because of informalities. Claims 24, 25, 27-32, 34, and 36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Barnett (U.S. Patent No. 6,772,157) in view of Schmuck (U.S. Patent No. 6,021,508). Claim 26 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Barnett in view of Schmuck, further in view of Anglin (U.S. Publ. No. 2004/0199521).[1]

The pending claims are directed to embodiments for delegating administrative rights in a zone based security system. Claim 24, for example, recites a method in a computer system wherein the computer system includes items stored in at least one volume, the volume being divided into at least one non-overlapping security zone, a security zone being defined as a grouping of items having common security rules. The method identifies first items for which common security rules are to be enforced and other items for which common security rules are to be maintained independent from the common security rules of the identified first items residing in a main non-overlapping security zone within a volume comprising a plurality of non-overlapping security zones. The main security zone is split into a first non-overlapping security zone containing the identified first items for which common security rules are to be enforced and a remaining non-overlapping main security having the other items having common security rules that are not dependent upon the common security rules of the first non-overlapping security zone such that the first non-overlapping security zone and the remaining non-overlapping main security zones do not overlap with any of the plurality of other non-overlapping security zones

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

included in the volume. The one or more main principals retain administrative rights for the first non-overlapping security zone and the remaining main non-overlapping security zone with the first non-overlapping security zone including the first items and the remaining main non-overlapping security zone including only the other items from the main non-overlapping security zone not included in the first items. The splitting is restricted in such a way as to prevent overlapping between security zones and such that none of the first items and other items from the main non-overlapping security zone are present in more than one security zone when the main non-overlapping security zone is split. The security zones thereby have a dynamic configurable granularity of items having common security rules. One or more first principals are then specified that also have administrative rights to the first non-overlapping security zone containing the first items, such that the entirety of items in the first non-overlapping security zone necessarily have the common security rules.

The remaining independent claim, claim 34, is a computer program product that contains elements generally corresponding to those in independent claim 24 described above. Accordingly, the discussion related to claim 24 is applicable to independent claim 34 as well.

The Office Action cites Barnett as teaching the delegation of administrative rights to sub-administrators in a method corresponding to claim 24. In Barnett, an administrator can delegate authority over a sub-domain of users to another administrator. Notably, however, because Barnett contains no teachings regarding non-overlapping zones, Schmuck is cited as disclosing identifying first items for which common security rules are to be enforced and other items for which common security rules are to be maintained independent from the common security rules of the identified first items; a first non-overlapping security zone of items having common security rules and a remaining non-overlapping main security zone having common security rules that are not dependent upon the common security rules of the first non-overlapping security zone such that the first non-overlapping security zone and the remaining non-overlapping main security zones do not overlap with any of the plurality of other non-overlapping security zones included in the volume; and that splitting is restricted in such a way as to prevent overlapping between security zones and such that none of the first items and other items from the main non-overlapping security zone are shared when the main non-overlapping security zone is split wherein the security zones thereby have a dynamic configurable granularity of items having common security rules.

Applicant respectfully disagrees with the assertion made in the Office Action regarding the teaching of Schmuck. Applicant respectfully submits that the teachings of Schmuck fail to disclose identifying items for which common security rules are to be enforced and splitting the security zone in such a way as to prevent overlapping between the security zones such that no items are shared between zones, as recited in combination with the other claims elements.

The cited art of Schmuck discloses the use of access control lists (ACL). As discussed in the background of the present applicant, one advantage of the present embodiments is that the security rules of items can be determined without using ACL's for each item. For instance, once a user has access to a security zone, access right lists no longer need to be determined when accessing each item within the zone, since the security rules are enforced to be consistent within the zone. Schmuck fails to teach such an element. Notably, while Schmuck, in column 28, states that there are typically groups of related files that all have the same access rights associated with them, nowhere is it found that the access rights are enforced as being the same for each related file. Furthermore, Schmuck does not disclose identifying the files, but instead discusses inheriting ACL's. Nowhere in Schmuck is there a limitation where the files necessarily have the same ACL's, only that it is unlikely that a user would associate a different ACL. By using the term "unlikely" it is clear that Schmuck anticipates that while unlikely, a user can change the ACL. Therefore, there is no enforcement of common rights among similar files. This is further supported by the lines 48-59 of column 28, where caching the ACL to allow lookups for **each** file because the ACL is likely to be cached in memory. Schmuck speeds up the process of checking ACL's, but does nothing to prevent the system from having to check the ACL for every file. This stands in contrast to the current embodiments, where the security rights are enforced for every item in a security zone, and only a single ACL lookup would need to be performed when accessing any number of items in the zone.

Furthermore, as previously noted and now clarified by the amendments of this response, one way in which a security zone varies from traditional security rules in that all items contained in a zone are required to have the same security rules. For example, while a directory may have security rules associated with the directory, each individual file underneath the directory has associated permissions that are allowed to differ from the parent directory. Therefore, even if access is allowed to a directory, the files in the directory may still be inaccessible depending on the individual permissions of the file. In the present invention, if the directory were in a security zone, once the security rules associate with the directory allow access to the zone, all items would be accessible because they necessarily have the same rights as the security zone. In other words, the claims recite that the zones would have the final determination as to security rights, where in the cited art the individual files could override a directory, zone, etc.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 31st day of October, 2008.

Respectfully submitted,

/Colby C. Nuttall, Reg. # 58146/

RICK D. NYDEGGER
Registration No. 28,651
COLBY C. NUTTALL
Registration No. 58,146
JOHN C. BACOCH
Registration No. 59,890
Attorneys for Applicant
Customer No. 047973

RDN:CCN:JCB:gd